REMARKS:

Claims 32-59 are currently pending. Claims 51-59 have been added with this response. Claims 32-34, 36-47, 49 and 50 stand rejected. The Examiner's indication of allowability with respect to claims 35 and 48 is gratefully acknowledged.

Claim 32 has been amended with this response to provide a definition for the variable *w*. This amendment has been made for clarification purposes only, since the Examiner has not objected to the claims on this basis.

Reconsideration of the Examiner's rejection of claims 32, 34, 36-46, 49 and 50 under 35 U.S.C. 102(b) as being anticipated by R. Silverman and D. Naccache, "Recent Results on Signature Forgery", RSA Laboratories Bulletin 11, April 1999 (Silverman et al.), is respectfully requested.

The Examiner is respectfully reminded that, in order to anticipate a claimed invention, a cited reference must clearly disclose each and every element of the claimed invention. In the present case, Silverman et al. does not clearly disclose the element of modulus C being selected from the group consisting of (a) w-big and w-heavy, and (b) w-little and w-light. Hence, Silverman et al. does not anticipate the presently claimed invention.

The terms w-big, w-heavy, w-little, and w-light are defined on Page 20 of the present specification for a w-bit number C. Thus, at Page 20, lines 4-5, a w-big number is said to be a number less than 2^w but close to 2^w. At Page 20, lines 8-9, a w-little number is said to be a number greater than 2^w but close to 2^w. At Page 20, lines 5-7, a w-heavy number is said to be a number less than 2^w but with a Hamming weight close to w. At Page 20, lines 9-11, a w-light number is said to be a number greater than 2^w but with a Hamming weight close to 1. At Page 25, Lines 1-2, the term "Hamming weight" is defined as the number of "1" bits in the binary representation of a number.

Turning now to the reference cited by the Examiner, Silverman et al. is concerned with security vulnerabilities in the ISO 9796 signature standard. In the section relied upon by the Examiner in his rejection, the reference identifies certain causes of this security vulnerability. For example, the reference notes that the security vulnerability exists only when the RSA

modulus is of the form $2^k \pm c$, where c is small. The reference notes that "such moduli are generally avoided because they may be ameniable (depending on c) to the special form of the Number Field Sieve and can be factored much faster than general integers of the same size. This is especially true in the case where c has low Hamming weight."

However, neither the portion of Silverman et al. cited by the Examiner, nor any other portion of that reference, contains a description that identifies the modulus described therein as having the properties of being w-big, w-little, w-heavy, or w-light. In this respect, Applicants note that claims 38-39 and 41-44, which separately claim the elements of the Markush group, have also been rejected as anticipated by Silverman et al., thus indicating that the Examiner is of the opinion that all of these features are taught by Silverman et al. Similar observations may be made with respect to the limitations of claims 34, 36, 40, 45, 46 and 49.

In the event that the Examiner is relying on an inherency argument with respect to these elements of the claimed invention, the Examiner is respectfully reminded of the dictates of M.P.E.P. 2112(IV), which require the Examiner to provide a rationale or evidence tending to show inherency:

> **IV. EXAMINER MUST PROVIDE RATIONALE OR EVIDENCE TENDING TO SHOW INHERENCY**
>
> The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) (reversed rejection because inherency was based on what would result due to optimization of conditions, not what was necessarily present in the prior art); *In re Oelrich*, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.' " *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (citations omitted) .... Also, "[a]n invitation to investigate is not an inherent disclosure" where a prior art reference "discloses no more than a broad genus of potential applications of its discoveries." *Metabolite Labs., Inc. v. Lab. Corp. of Am. Holdings*, 370 F.3d 1354, 1367, 71 USPQ2d 1081, 1091 (Fed. Cir. 2004) (explaining that "[a] prior art reference that discloses a genus still does not inherently disclose all species within that broad category" but must be examined

> to see if a disclosure of the claimed species has been made or whether the prior art reference merely invites further experimentation to find the species.<
>
> "In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art." *Ex parte Levy*, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (emphasis in original)

In the present case, the Examiner has failed to provide a rationale or evidence tending to show inherency. Indeed, the Examiner has not even used the term "inherency" in setting forth the present rejection. Rather, Applicants are led to consider the possibility of inherency only because there is no clear teaching of the cited claim elements in the reference cited by the Examiner. It is thus respectfully requested, if the Examiner intends to maintain the present rejection and if that rejection is based on an inherency argument, that the Examiner specifically state so on the record and provide an appropriate rationale or evidence. Moreover, if such is the case, the Examiner is respectfully requested to make the following Office Action non-final, since Applicants have been placed in a position where they are unable to adequately respond to the Examiner's rejection due to the failure of the Examiner to clearly set forth the grounds thereof.

Reconsideration of the Examiner's rejection of claims 33 and 47 under 35 U.S.C. 103(a) and being unpatentable over R. Silverman and D. Naccache, "Recent Results on Signature Forgery", RSA Laboratories Bulletin 11, April 1999 (Silverman et al.) in view of A. Menezes, P. Oorschot, and S. Vanstone, "Handbook of Applied Cryptography", CRC Press LLC, 1997 (Menezes et al.) is respectfully requested.

The Examiner is respectfully reminded that, in establishing a prima facie case of obviousness, the Examiner may not pick and choose among the teachings of a reference, taking only those elements that support a given position, while disregarding other elements which teach away from it. Rather, a reference must be construed as a whole for what it fairly suggests to one skilled in the art. Moreover, the Examiner is respectfully reminded that a case of prima facie obviousness cannot be established in circumstances where one skilled in the art would lack proper incentive to combine or modify the teachings of the cited prior art.

The Examiner is also respectfully reminded of the diverse requirements of 35 U.S.C. § 102 and 35 U.S.C. § 103. In particular, while a novelty inquiry seeks to ascertain the existence

of each of the claimed elements in a cited reference, an obviousness inquiry contains the additional element of incentive (i.e., incentive to modify or combine). For this reason, it is possible for a reference to raise issues with respect to the novelty of a claimed invention, without raising issues with respect to the obviousness of a claimed invention. Of particular relevance here, this may happen, for example, where a reference teaches away from an invention. In that case, the reference may be problematic from a bare novelty standpoint, but is no longer a bar to patentability when the invention has been claimed in such a way that it is novel over the reference. Indeed, in that circumstance, the reference is often strong evidence of the patentability of the claimed invention.

In the present case, Silverman et al. is concerned with security vulnerabilities in the ISO 9796 signature standard. In the section relied upon by the Examiner in his rejection, the reference identifies certain causes of this security vulnerability. For example, the reference notes that the security vulnerability exists only when the RSA modulus is of the form $2^k \pm c$, where c is small. The reference notes that "such moduli are generally avoided because they may be ameniable (depending on c) to the special form of the Number Field Sieve and can be factored much faster than general integers of the same size. This is especially true in the case where c has low Hamming weight."

It is thus clear from the foregoing that, when Silverman et al. is construed as a whole for what it fairly suggests to one skilled in the art, the reference actually teaches away from the use of such aforementioned moduli. Thus, given the teachings of Silverman et al., one skilled in the art would have no incentive to encrypt data using such moduli, because the resulting data would have precisely the sort of security vulnerability that Silverman et al. warns against. Menezes et al. does nothing to cure this infirmity, and indeed, appears to have been cited by the Examiner solely for its teachings regarding mixed radix systems.

Put another way, even if Menezes et al. contains the teachings that the Examiner is ascribing to it, the combination of Silverman et al. with Menezes et al. does not teach the present invention as it must in order to support a rejection under 35 U.S.C. § 103. To the contrary, Silverman et al. clearly teaches that moduli of the form $2^k \pm c$, where c has low Hamming weight, present a security vulnerability. Hence, any system resulting from the combination of the teachings of these references would specifically avoid the use of such moduli.

Atty. Docket No.: LYRN002US0
Customer ID No. 58,293

Should the Examiner have any questions or desire clarification of any sort, the Examiner is invited to telephone the undersigned at the number listed below. Please reference Attorney Docket No. LYRN002US0.

A Fee Transmittal is submitted herewith indicating that no further fee is due with this transmission due to a higher number of claim fees being previously paid. However, if a fee is due or a credit deemed appropriate, the Commissioner is hereby authorized to debit or credit Deposit Account No. 50-3694 of Fortkort & Houston P.C. accordingly.

Respectfully submitted,
FORTKORT & HOUSTON P.C.

Date: September 19, 2006

By: _____
John A. Fortkort
Reg. No. 38,454
ATTORNEY FOR APPLICANTS

9442 N. Capital of Texas Hwy.
Arboretum Plaza One, Suite 500
Austin, Texas 78759
Tel: (512) 343-4525
Fax: (512) 343-4530
Jfortkort@foholaw.com